AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

~~The present invention~~[0020.5] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction and translation logic. The cryptographic instruction is received by fetch logic in a microprocessor ~~by a computing device~~ as part of an instruction flow executing on the ~~computing device~~microprocessor. The cryptographic instruction is retrieved from memory and prescribes one of the cryptographic operations. The translation logic is operatively coupled to the cryptographic instruction. The translation logic translates the cryptographic instruction into micro instructions, where the micro instructions are ordered to direct the ~~computing device~~ microprocessor to load a second input text block from the memory and to execute the one of the cryptographic operations on the second input text block prior to directing the ~~computing device~~ microprocessor to store an output text block corresponding to a first input text block to the memory. Consequently, the output text block is stored during execution of the one of the cryptographic operations on the second input text block.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has fetch logic, and translation logic that is configured to translate a cryptographic instruction into a sequence of micro instructions. The fetch logic is disposed within a microprocessor, and is configured to fetch a cryptographic instruction from memory as part of an instruction flow executing on the microprocessor. The cryptographic instruction directs the microprocessor to perform one of the cryptographic operations. The sequence of micro instructions includes a first micro instruction and a second micro instruction. The first micro instruction directs that

a second input text block be loaded from the memory and that one of the cryptographic operations be executed on the second input text block. The second micro instruction directs that a first output text block be stored to the memory, where the first output text block corresponds to a first input text block upon which the one of the cryptographic operations is executed. The translation logic issues the first micro instruction prior to issuing the second micro instruction.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations ~~in a device~~. The method ~~includes~~ includes, within a microprocessor, fetching a cryptographic instruction from a memory as part of an instruction flow executing on the microprocessor; wherein the cryptographic instruction prescribes one of the cryptographic operations; ~~translating a~~ translating the cryptographic instruction ~~that prescribes execution of one of the cryptographic operations~~ into a first micro instruction and a second micro instruction, the first micro instruction directing the ~~device~~ microprocessor to load a second input text block ~~be loaded~~ from the memory and to execute the one of the cryptographic operations on the second input text block, the second micro instruction directing the ~~device~~ microprocessor to store a first output text block to the memory, where the first output text block corresponds to a first input text block upon which the one of the cryptographic operations is executed; and issuing the first micro instruction to a cryptography unit within the microprocessor prior to issuing the second micro instruction to the cryptography unit; whereby the issuing causes the output text block to be stored during execution of the one of the cryptographic operations on the second input text block.